UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Records and information associated with the cellular device assigned (414) 315-4416, that is in the custody or control of US Cellular, as further described in Attachment A

Case No. 23 MJ 63

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☐ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☑ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 1349 & 1341	Conspiracy to commit mail fraud and mail fraud.

The application is based on these facts:

See Attached Affidavit.

- ☑ Continued on the attached sheet.
- ☑ Delayed notice of 30 days *(give exact ending date if more than 30 days: _____)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

FBI SA David Shamsi
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 5/1/2023

Judge's signature

City and state: Milwaukee, Wisconsin

Honorable William E. Duffin, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, David Shamsi, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND BACKGROUND

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c) to authorize law enforcement to employ electronic investigative techniques, as described in the following attachment, to determine the location of the target cellular device assigned call number (414) 315-4416, whose service provider is US Cellular ("Service Provider") a wireless telephone service provider headquartered at 8410 W Bryn Mawr Ave, Chicago, Illinois, referred to in this affidavit as the "Target Cellular Device." This affidavit is made in support of up to two different search warrants to locate the phone: 1) by obtaining information from the service provider, e.g., cell site and other precision location information and/or 2) by utilizing a device that acts as a cell phone tower sometimes referred to as a Cell Site Simulator or Wi-Fi geolocation device. In addition, because this request may be construed as a Pen Register/Trap and Trace device or request, the application for this warrant (which includes this affidavit) is intended to comply with 18 U.S.C. § 3122.

2. I am a Special Agent with the Federal Bureau of Investigation and have experience in the investigation, apprehension and prosecution of individuals involved in federal criminal offenses, the use of cellular devices to commit those offenses and the

available technology that can be used by law enforcement to assist in identifying the users of cellular devices and their location.

3. The facts in this affidavit come from my personal observations, training, experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. There is reason to believe the target cellular device is currently located in this district. The user of the Target Cellular Device, identified as Michael Anderson, is known to spend most of their time in the Eastern District of Wisconsin. Michael Anderson resides in the Eastern District of Wisconsin and has been observed via physical surveillance in Milwaukee, Wisconsin as of April 28, 2023.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that Michael Anderson is using the Target Cellular Device. Based on the facts set forth in this affidavit, there is probable cause to believe that Anderson has violated Section 18, United States Code, Sections 1341 & 1349 (mail fraud and conspiracy to commit mail fraud). Anderson was charged with these crimes on April 25, 2023 and Anderson is the subject of an arrest warrant issued on April 26, 2023. There is also probable cause to believe that the location information described in Attachment B will assist law enforcement in arresting Anderson, who is a "person to be arrested" within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

COVID-19 Pandemic Unemployment Assistance Fraud

6. On March 13, 2020, the President of the United States declared COVID-19 an emergency under the Robert T. Stafford Disaster Relief and Emergency Assistance Act. Congress subsequently passed the Coronavirus Aid, Relief, and Economic Security Act ("CARES ACT"), which was signed into law by the President on March 27, 2020. The CARES act provided over $2 trillion in economic relief protections to the American people from the public health and economic impacts of COVID-19.

7. Since 1935, the U.S. Department of Labor's Unemployment Insurance (UI) program has provided unemployment benefits to eligible workers who become unemployed through no fault of their own. This program was enacted to provide financial assistance to eligible workers while they sought employment. UI beneficiaries who meet the requirements of the applicable state law are eligible for this temporary financial assistance. Each state administers a separate UI program within the guidelines established by federal law.

8. The CARES Act established a new program—Pandemic Unemployment Assistance (PUA)—to provide unemployment benefits during the COVID-19 pandemic to people who do not qualify for regular unemployment insurance benefits including business owners, self-employed workers, independent contractors, and those with a limited work history who are out of business or have significantly reduced their services as a direct result of the pandemic. Unemployment insurance benefits provided under the

PUA program are sometimes referred to as PUA benefits. Each state's unemployment insurance office is responsible for distributing these benefits if available in that state.

9. In California, the state entity responsible for administering and providing UI and PUA benefits, is known as the Employment Development Department (EDD). After submitting a claim and being approved for these benefits, the EDD would send a prepaid debit card to the eligible worker's residence, which would be preloaded with a pre-determined amount of money depending on the individual claimant's application.

10. To submit a claim with the EDD, individuals must first create an account and verify their identity using the website, ID.me. ID.me provides secure identity proofing, authentication, and group affiliation verification for government and businesses across sectors. The ID.me secure digital identity network has over 100 million members, as well as partnerships with 31 states, multiple federal agencies, and over 500 name brand retailers. Each ID.me participating entity sets the level of identity verification required to access their products, services, and/or benefits. To access EDD benefits, claimants must register with ID.me through one of two ways: self-verification or video call. To register via self-verification, an individual must upload a photograph of either a driver's license, state ID, passport, or passport card, as well as a "video selfie," and then provide their social security number. To register via video call, an individual can enter their social security number into the system and then show their driver's license, state ID, passport, or passport card to an ID.me representative during a recorded

video call, who then compares the identification photograph to the call participant to confirm the individual's identity.

Wild 100s Investigation

11. Since June of 2020, the Federal Bureau of Investigation (FBI), in coordination with the Milwaukee Police Department (MPD) and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), has been investigating identified members of the violent street gang, Wild 100s, for federal firearms offenses and drug offenses. While investigating these crimes, law enforcement observed numerous social media posts by Wild 100s members indicating the gang was engaged in multiple schemes to fraudulently obtain UI and PUA benefits and began investigating members of the gang for engaging in mail fraud and conspiracy to commit mail fraud.

12. During the review of the Instagram, case agents identified several instances of the unemployment insurance fraud being committed by Michael Anderson, a Wild 100s member. One example was Anderson talking to username "fallfor_mee", identified as Amanda Oberg (DOB XX/XX/1997). Anderson asks Oberg for her demographics, such as her social security number, date of birth, phone number and address. Anderson sent a screenshot of an "id.me" identification verification page which showed Oberg's driver's license which was submitted online to create a California Unemployment Insurance application. Below are screenshots of the communications.

13. Additionally, the Instagram account tracked log ins through specific IP addresses and case agents determined that Anderson logged in to IP address

76.30.226.248 to access his account. The IP address 76.30.226.248 was also the same IP used to submit unemployment claims for 35 individuals which case agents identified as fraudulent. Furthermore, the IP address was also accessed by other co-conspirators and Wild 100s gang members, Chase Nanez, Ronnell Bowman, and Joel Blake to submit fraudulent unemployment applications.

14. It should be noted that almost all the 35 applications for unemployment were submitted alleging that the previous employer for each applicant was "True Barber" with a previous supervisor of "Johnathan Young". Case agents know through the course of the investigation that each member of the gang was instructed to use a barber shop or cosmetology profession to apply for benefits since the face-to-face contact is more likely to get applications approved without issues.

15. In September 2022, law enforcement had contact with victim J.K. regarding a vehicle theft for which Michael Anderson was the suspect and is now charged in Waukesha County Circuit Court. J.K. provided law enforcement with the phone number of 414-315-4416 (Target Cellular Device) as the number of Michael Anderson, who she identified as the individual who stole her car. J.K. stated that J.K. contacted Anderson via the Target Cellular Device to purchase drugs and that Anderson stole her vehicle as payment for drugs.

16. On or about December 16, 2022, a pen register trap and trace (PRTT) order was issued in the Eastern District of Wisconsin, directing Instagram to provide the FBI

with real-time collection of subscriber and transactional data associated with the Instagram account, ikey4blk.

17. Upon reviewing toll records obtained for the Target Cellular Device there were multiple contacts between Anderson and Ronnell Bowman (his brother), Quevon McKinnie, and Vernell Hamilton, all of which are Wild 100s aka Shark Gang members. The Target Cellular Device was in frequent communication with Jontwon Anderson, a known Wild 100s aka Shark Gag member and Michael Anderson's brother, as recently as April 27, 2023.

AUTHORIZATION REQUEST & MANNER OF EXECUTION

18. I request that the Court issue the proposed search warrant pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. §§ 2703(c) and 2711.

19. Because collecting the information authorized by this warrant may fall within the statutory definitions of a "pen register" or a "trap and trace device," *see* 18 U.S.C. § 3127(3) & (4), this application and the accompanying warrant are intended to comply with requirements set forth in 18 U.S.C. §§ 3122-3123.

20. In my training and experience, I have learned that cellular phones and other cellular devices communicate wirelessly across a network of cellular infrastructure, including towers that route and connect individual communications. When sending or receiving a communication, a cellular device broadcasts certain signals to the cellular tower that is routing its communication. These signals include a cellular device's unique identifiers.

21. In my training and experience, I have learned that US Cellular, is a wireless service provider with its headquarters located within the United States and provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of cellular devices to which they provide service. That information includes (1) E-911 Phase II data, also known as GPS data or latitude-longitude data, (2) cell-site data, also known as "tower/face information" or cell tower/sector records, and (3) timing advance or engineering data commonly referred to as per call measurement data (RTT, True Call, LDBoR, or equivalent). E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device's signal using data from several of the provider's cell towers. Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device.

22. To facilitate execution of this warrant, law enforcement may use an investigative device or devices (sometimes referred to as a Cell Site Simulator or Wi-Fi geolocation device) capable of broadcasting signals that will be received by the Target

Cellular Device or receiving signals from nearby cellular devices, including the Target Cellular Device. Such a device may function in some respects like a cellular tower, except that it will not be connected to the cellular network and cannot be used by a cell phone to communicate with others. The device may send a signal to the Target Cellular Device and thereby prompt it to send signals that include the unique identifier of the device. Law enforcement may monitor the signals broadcast by the Target Cellular Device and use that information to determine the Target Cellular Device's location, even if it is located inside a house, apartment, or other building.

23. The investigative device may interrupt cellular service of phones or other cellular devices within its immediate vicinity. Any service disruption to non-target devices will be brief and temporary, and all operations will attempt to limit the interference with such devices. In order to connect with the Target Cellular Device, the device may briefly exchange signals with all phones or other cellular devices in its vicinity. These signals may include cell phone identifiers. The device will not complete a connection with cellular devices determined not to be the Target Cellular Device, and law enforcement will limit collection of information from devices other than the Target Cellular Device. To the extent that any information from a cellular device other than the Target Cellular Device is collected by the law enforcement device, law enforcement will delete that information, and law enforcement will make no investigative use of it absent further order of the court, other than distinguishing the Target Cellular Device from all other cellular devices.

24. I request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 30 days after the collection authorized by the warrant has been completed. This delay is justified because there is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of the target cellular device would seriously jeopardize the ongoing investigation. Such disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). There is a reasonable necessity for the use of the techniques described. *See* 18 U.S.C. § 3103a(b)(2). As further specified in the attachment, which is incorporated into the warrant, the proposed search warrant does not authorize the seizure of any tangible property. *See* 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is a reasonable necessity for that seizure. *See* 18 U.S.C. § 3103a(b)(2).

25. I further request the following information from the service provider: the installation and use of a pen register trap and trace device, beginning 30 days from the date the warrant is issued.

26. I further request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the target cellular device

outside of daytime hours.

27. I further request that the pen register / trap and trace device be transferable to any changed dialed number subsequently assigned to a device bearing the same ESN, IMSI, or SIM as the Target Cellular Device; any changed ESN, IMSI, or SIM subsequently assigned the same dialed number as the Target Cellular Device; or any additional changed dialed number, ESN, IMSI, or SIM listed to the same subscriber account as the Target Cellular Device.

28. A search warrant may not be legally necessary to authorize all of the investigative techniques described. Nevertheless, I submit this warrant application out of an abundance of caution.

ATTACHMENT A

This warrant authorizes the use of the electronic investigative technique described in Attachment B to identify the location of the cellular device assigned phone number (414) 315-4416 (Target Cellular Device), whose service provider is US Cellular ("Service Provider") a wireless telephone service provider headquartered at 8410 W Bryn Mawr Ave, Chicago, Illinois.

This Warrant also serves as a Pen Register order under 18 U.S.C. § 3123. The Court makes the following findings: Michael Anderson is the person to whom the pen register or trap and trace device are to be attached/applied and who is the subject of the criminal investigation; (414) 315-4416 is the phone number to which the device is to be attached; and Title 18, United States Code, Sections 1341 and 1349 (mail fraud and conspiracy to commit mail fraud) are the offenses, to which information relates; and

The attorney for the government has certified to this Court that the information likely to be obtained by the installation and use of the pen register or trap and trace device is relevant to an ongoing criminal investigation by the Federal Bureau of Investigation.

ATTACHMENT B

Particular Things to Be Seized

with a Cell Site Simulator or Wi-Fi Geolocation Device

This Warrant authorizes the officers to whom it is directed to determine the location of the target cellular device by collecting and examining:

1. radio signals emitted by the target cellular device for the purpose of communicating with cellular infrastructure, including towers that route and connect individual communications; and
2. radio signals emitted by the target cellular device in response to signals sent to it by the officers;

for a period of thirty (30) days, during all times of day and night. This includes monitoring non-content signaling and routing information, including all non-content packet switched data, through the installation and use of a pen register and trap and trace device pursuant to 18 U.S.C. § 3123 by the Federal Bureau of Investigation. Because the use of the device, a Cell Site Simulator or Wi-Fi geolocation device, may fall within the definitions of a "pen register" or a "trap and trace device," see 18 U.S.C. § 3127(3) & (4), the application and the warrant are designed to comply with the Pen Register Statute as well as Rule 41. The application therefore includes all information required for and serves as a pen register application, 18 U.S.C. § 3123(a); similarly, the warrant therefore includes all the information required for and serves as a pen register order, 18 U.S.C. § 3123(b).

This warrant does not authorize the interception of any content (telephone, text message, or internet based). The investigative device may interrupt cellular service of phones or other cellular devices within its immediate vicinity. Any service disruption to non-target devices will be brief and temporary, and all operations will attempt to limit the interference with such devices. In order to connect with the Target Cellular Device, the device may briefly exchange signals with all phones or other cellular devices in its vicinity. These signals may include cell phone identifiers. The device will not complete a connection with cellular devices determined not to be any of the Target Cellular Device, and law enforcement will limit collection of information from devices other than the Target Cellular Device. To the extent that any information from a cellular device other than the Target Cellular Device is collected by the law enforcement device, law enforcement will delete that information, and law enforcement will make no investigative use of it absent further order of the court, other than distinguishing the Target Cellular Device from all other cellular devices.

Under this warrant, the cell site simulator/geolocation device shall be transferable to any changed dialed number subsequently assigned to a device bearing the same ESN, IMSI, or SIM as the Target Cellular Device; any changed ESN, IMSI, or SIM subsequently assigned the same dialed number as the Target Cellular Device; or any additional changed dialed number, ESN, IMSI, or SIM listed to the same subscriber account as the Target Cellular Device.

The Court finds reasonable necessity for use of the techniques and collection of information described. *See* 18 U.S.C. § 3103a(b)(2).

This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the information described. *See* 18 U.S.C. § 3103a(b)(2).

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ❒ Original ❒

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
The location of the target cellular device assigned call number (414) 315-4416, whose service provider is US Cellular, as further described in Attachment A

Case No. 23 MJ 63

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 5/14/2023 *(not to exceed 14 days)*

❒ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. William E. Duffin.
(United States Magistrate Judge)

☑ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☑ for 30 days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____.

Date and time issued: 5/1/2023 at 3:34 PM

William E. Duffin
Judge's signature

City and state: Milwaukee, Wisconsin

Honorable William E. Duffin, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

This warrant authorizes the use of the electronic investigative technique described in Attachment B to identify the location of the cellular device assigned phone number (414) 315-4416 (Target Cellular Device), whose service provider is US Cellular ("Service Provider") a wireless telephone service provider headquartered at 8410 W Bryn Mawr Ave, Chicago, Illinois.

This Warrant also serves as a Pen Register order under 18 U.S.C. § 3123. The Court makes the following findings: Michael Anderson is the person to whom the pen register or trap and trace device are to be attached/applied and who is the subject of the criminal investigation; (414) 315-4416 is the phone number to which the device is to be attached; and Title 18, United States Code, Sections 1341 and 1349 (mail fraud and conspiracy to commit mail fraud) are the offenses, to which information relates; and

The attorney for the government has certified to this Court that the information likely to be obtained by the installation and use of the pen register or trap and trace device is relevant to an ongoing criminal investigation by the Federal Bureau of Investigation.

ATTACHMENT B

Particular Things to Be Seized

with a Cell Site Simulator or Wi-Fi Geolocation Device

This Warrant authorizes the officers to whom it is directed to determine the location of the target cellular device by collecting and examining:

1. radio signals emitted by the target cellular device for the purpose of communicating with cellular infrastructure, including towers that route and connect individual communications; and
2. radio signals emitted by the target cellular device in response to signals sent to it by the officers;

for a period of thirty (30) days, during all times of day and night. This includes monitoring non-content signaling and routing information, including all non-content packet switched data, through the installation and use of a pen register and trap and trace device pursuant to 18 U.S.C. § 3123 by the Federal Bureau of Investigation. Because the use of the device, a Cell Site Simulator or Wi-Fi geolocation device, may fall within the definitions of a "pen register" or a "trap and trace device," see 18 U.S.C. § 3127(3) & (4), the application and the warrant are designed to comply with the Pen Register Statute as well as Rule 41. The application therefore includes all information required for and serves as a pen register application, 18 U.S.C. § 3123(a); similarly, the warrant therefore includes all the information required for and serves as a pen register order, 18 U.S.C. § 3123(b).

This warrant does not authorize the interception of any content (telephone, text message, or internet based). The investigative device may interrupt cellular service of phones or other cellular devices within its immediate vicinity. Any service disruption to non-target devices will be brief and temporary, and all operations will attempt to limit the interference with such devices. In order to connect with the Target Cellular Device, the device may briefly exchange signals with all phones or other cellular devices in its vicinity. These signals may include cell phone identifiers. The device will not complete a connection with cellular devices determined not to be any of the Target Cellular Device, and law enforcement will limit collection of information from devices other than the Target Cellular Device. To the extent that any information from a cellular device other than the Target Cellular Device is collected by the law enforcement device, law enforcement will delete that information, and law enforcement will make no investigative use of it absent further order of the court, other than distinguishing the Target Cellular Device from all other cellular devices.

Under this warrant, the cell site simulator/geolocation device shall be transferable to any changed dialed number subsequently assigned to a device bearing the same ESN, IMSI, or SIM as the Target Cellular Device; any changed ESN, IMSI, or SIM subsequently assigned the same dialed number as the Target Cellular Device; or any additional changed dialed number, ESN, IMSI, or SIM listed to the same subscriber account as the Target Cellular Device.

The Court finds reasonable necessity for use of the techniques and collection of information described. *See* 18 U.S.C. § 3103a(b)(2).

This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the information described. *See* 18 U.S.C. § 3103a(b)(2).